# Policy

## Information Security

NSWHP_PD_033

## 1. Purpose

This policy mandates the implementation of a secure environment for the systems that NSW Health Pathology (NSWHP) manages, and the data it processes. NSWHP deals with sensitive personal and health data as part of its day-to-day business. NSWHP is dedicated to applying information security consistently and sustainably to ensure the confidentiality, integrity, and availability (CIA) of the information it processes and the digital assets it maintains. Information security is a key consideration in delivering our services and our commitment to information security will allow us to continue to safely and reliably meet stakeholder needs.

## 2. Background

The NSW Cyber Security Policy (CSP) requires NSW Government agencies to implement and maintain an Information Security Management System (ISMS). The NSWHP ISMS is designed around a mature framework to ensure information security is applied consistently and in a measurable method to allow for continuous improvement, in accordance with ISO/IEC 27001:2022.

A core focus of the ISMS will be to secure NSWHP systems through compliance with the requirements of the Essential 8 and the Mandatory 20 as set out in the CSP.

## 3. Scope

This policy applies to all NSW Health Pathology staff, contractors (including visiting practitioners, recruitment agency staff and volunteers) working within or for NSWHP, and students, researchers or anyone else undertaking or delivering training, education or research in NSWHP, as well as the information and systems they manage as outlined below. The key focus of this policy is to protect information; the format or way in which it is handled is secondary. Instances of information outside of a digital system or format should not be assumed as out of scope.

| Logical | Physical |
|---|---|
| • Corporate and Forensic and Analytical Science Service (FASS) public-facing systems, supporting infrastructure and data<br>• All NSWHP Crown Jewels<br>• NSWHP managed processes that transfer sensitive data to services providers or third parties | • Corporate:<br>  • Level 2, 1 Reserve Road, St Leonards, NSW, 2065<br>  • Level 5, 45 Watt Street, Newcastle NSW, 2300<br>• FASS:<br>  • 480 Weeroona Road, Lidcombe NSW, 2141<br>  • 1A Main Avenue, Lidcombe, NSW, 2141<br>  • John Hunter Hospital Campus, Rosella Close, New Lambton NSW 2305<br>  • Wollongong Hospital, Level 2 Block A Loftus Street, Wollongong NSW 2500<br>  • Cameron Building, Macquarie Hospital, Badajoz Road, North Ryde NSW 2113 |

Exclusions:

- Local Health District supplied infrastructure and systems
- eHealth supplied infrastructure and systems

## 4. Definitions

**Crown Jewel:** The most valuable or operationally vital systems or information in an organisation - NSWHP Crown Jewels are recorded in the Crown Jewel Register

**Crown Jewel Register:** A managed list of NSWHP digital assets along with supporting information used to determine the assets criticality

**DIGS:** Data and Information Governance Steering Committee

**Digital Asset:** A component which stores or processes one or more Information Assets

**Essential Eight:** Eight mitigation controls released by the Australian Signals Directorate's Australian Cyber Security Centre and classified as essential to help reduce the likelihood and impact of a cyber security breach

**Information Asset:** A discrete collection of data or information, stored in any manner, which is recognised as having value and is required to be managed by the organisation

**Information Security:** The preservation of confidentiality, integrity and availability of information (ISO 27000)

**ISWG:** Information Security Working Group - manages matters regarding the ISMS and advises the Data and Information Governance Steering Committee

**Mandatory 20:** The 20 mandatory requirements in the NSW Cyber Security Policy

**Top management:** A term used in ISO 27001 to refer to the equivalent of NSW Health Pathology's Strategic Leadership Team (SLT)

## 5. Policy Statement

### Principles

A guiding principle used in information security at NSWHP is to maintain the CIA triad:

- Confidentiality - Handling of information to ensure that it will not be disclosed in ways that are inconsistent with authorised use and its original purpose (PD2020_046 Electronic Information Security)
- Integrity - To protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity (PD2020_046 Electronic Information Security)
- Availability - Ensuring timely and reliable access to and use of information (PD2020_046 Electronic Information Security)

The outcome of a focus on the CIA triad will be improved patient safety, compliance with legislation and policies and an ability to innovate safely and sustainably. It will also contribute to and enhance patient, stakeholder and community confidence in the security of NSWHP systems and data.

This Policy is the foundation of the ISMS and is supported by other ISMS topic-specific standards, procedures and documents that should be considered as a whole and not in isolation. These documents include but are not limited to information security risk management, information security incident management, secure software development and project implementation.

### Security Objectives

This policy supports the following security objectives of NSWHP:

| Objective | Action | Measurement |
|---|---|---|
| **Improve information security posture through compliance** | Maintain compliance and alignment with:<br>• State and federal legislation as defined in the NSWHP Compliance Register<br>• NSW Health Information security policies | • Annual Cyber Security NSW Maturity Attestation (Essential Eight and Mandatory 20)<br>• ISO 27001 Audits (Internal and external)<br>• Internal security reviews |
| **Certification** | Gain and maintain ISO 27001 certification | Audit results and certificate when achieved |
| **Develop Information security awareness and a cyber security culture** | Consistently engage staff and leverage the communications teams' channels to raise awareness of information security<br>Conduct targeted campaigns designed to raise awareness through tabletop exercises, phishing campaigns and other simulations<br>Ensure staff information security training is attended and appropriate | • Monitor staff engagement with training material<br>• Monitor results of simulation outcomes<br>• Monitor compliance with training requirements<br>• Monitor engagement with security exercises |

NSWHP will take a risk-based approach to information security ensuring decisions align with the Risk Appetite endorsed by the NSWHP Board.

When evaluating risks and controls, guidance provided by eHealth NSW, the NSW Ministry Of Health, Cyber Security NSW, and the Australian Signals Directorate's Australian Cyber Security Centre will be taken into consideration. The Australian Information Security Manual represents a wealth of knowledge and in the absence of local policy, it should be used to drive decisions where possible.

The ISMS will continually evolve, being driven by new legislative and policy requirements as well as feedback from audits and learnings taken from the review of security incidents and events.

**Interested Parties**

The ISMS scope considers the requirements of the following interested parties outside of NSWHP and its patients:

- NSW Ministry of Health:
  - eHealth NSW
  - Cancer Institute NSW
  - Local Health Districts
- NSW Department of Communities & Justice
- National Cancer Screening Register
- National Notifiable Diseases Surveillance Systems
- Cyber Security NSW
- Australian State and Federal Government

**Issues**

The potential to achieve the information security objectives, and effectively leverage the benefits of the ISMS may be impacted by the following:

- Resource constraints
- Broad distribution of NSWHP staff and systems both geographically and across LHD / eHealth boundaries
- Dependency on policies and procedures developed outside of the ISMS or NSWHP’s scope of influence
- Pre-existing contracts and legacy systems where the organisation does not have the appetite or ability to change

## 6. Roles and Responsibilities

- The Data and Information Governance Steering Committee has oversight over the ISWG, ISMS and NSWHP's information security responsibilities as outlined in the committee's terms of reference
- The Information Security Working Group (ISWG) is responsible for
  - The development, review and endorsement of ISMS documentation and procedures and the implementation of the ISMS
  - Meeting monthly to review risks, monitor the effectiveness of the ISMS and review security events
  - Additional responsibilities as outlined in the Information Security Working Group Terms of Reference

- The Chief Information Officer shall act as the owner of the ISMS and is responsible for the successful operation of the ISMS throughout NSWHP
- The Chief Security Architect shall be responsible for chairing the ISWG, maintaining ISMS documentation, coordinating annual risk assessments, audits, and security reviews, and responding to the direction of the ISMS owner
- The NSWHP Strategic Leadership Team (Top Management) will ensure appropriate organisational commitment and resourcing to information security activities related to the scope of the ISMS
- Information Asset Owners are responsible for:
    - assessing the value of Information Assets and classifying their criticality and sensitivity
    - conducting annual risk assessments
    - resourcing the establishment and sustainment of appropriate controls to safeguard the Information Assets

## 7. Legal and Procedure Framework

### 7.1 Related Procedure Document Suite

PD2015_049 NSW Health Code of Conduct
PD2009_076 Communications - Use & Management of Misuse of NSW Health Communications Systems
NSW Health Electronic Information Security Policy Directive
NSW Health Privacy Manual for Health Information
NSWHP Compliance Management Framework
NSW Health Enterprise-wide Risk Management Policy Directive

### 7.2 Related Legislation and Supporting Documents

NSW Privacy and Personal Information Protection Act
NSW Health Records and Information Privacy Act 2002
NSW Classification and Labelling Guideline
NSW Cyber Security Policy
ACSC Strategies to Mitigate Cyber Security Incidents
ISO/IEC 27001:2022 Information security management standard
ISO/IEC 27002:2022 Code of practice for information security controls
ISO/IEC 27003:2017 Information Security Management Systems - Guidance

## 8. Review

This policy will be reviewed annually. The next review will be completed by 1/06/2024

## 9. Risk

| | |
|---|---|
| **Risk Statement** | Compliance with this policy will ensure that NSW Health Pathology operates its information assets safely and securely in line with legislative requirements. It will enable the development of an ISMS that will reduce our risk exposure to information security threats. |
| **Risk Category** | Leadership and Management |

## 10. Further Information

For further information, please contact:

| | |
|---|---|
| **Policy Contact Officer** | Position: Chief Security Architect |
| | Name: Desmond Horsley |
| | Email: desmond.horsley@health.nsw.gov.au |

## 11. Version History

The approval and amendment history for this document must be listed in the following table.

| Version No | Effective Date | Approved By | Approval Date | Procedure Author | Risk Rating | Sections Modified |
|---|---|---|---|---|---|---|
| 1.0 | 17/07/2023 | SLT | 04/07/2023 | Chief Security Architect | High | New Policy |